AULA

Irredutibilidade em $\mathbb{Q}[x]$

4

META:

Fundamentar a busca de critérios de irredutibilidade em $\mathbb{Z}[x]$ para mostrar irredutibilidade em $\mathbb{Q}[x]$.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Definir polinômios primitivos em $\mathbb{Z}[x]$.

Enunciar o lema de Gauss.

Mostrar que um polinômio primitivo é irredutível em $\mathbb{Z}[x]$ se e somente se é irredutível em $\mathbb{Q}[x]$.

PRÉ-REQUISITOS

As definições de raiz de polinômio, máximo divisor comum e elemento irredutível.

4.1 Introdução

Nesta aula, restringiremos nosso estudo de polinômios ao conjunto $\mathbb{Q}[x]$. Focalizaremos sobre os elementos irredutíveis. Pela relação entre redutibilidade e existência de raízes, começaremos por caracterizar as raízes racionais de um polinômio em $\mathbb{Q}[x]$. Este é o teste da raiz racional. Na seção 4.2, abordaremos o conceito de conteúdo de um polinômio com coeficientes inteiros e provaremos o resultado fundamental a cerca deste; a saber: o teorema de Gauss. Na seção que segue, provaremos o lema de Gauss, nosso principal resultado desta aula. Finalmente, fecharemos a aula colhendo o fruto de tanto esforço. Concluiremos que irredutibilidade em $\mathbb{Q}[x]$ pode ser obtida por meio de irredutibilidade em $\mathbb{Z}[x]$.

4.2 Teste da raiz racional

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ um polinômio de grau $n \geq 1$. Seja $\frac{r}{s}\mathbb{Q}$ uma raiz não nula de $f(x)$. Podemos assumir $\frac{r}{s}$ nos menores termos, isto é, MDC $(r, s) = 1$. Por definição de raiz,

$$f(\frac{r}{s}) = a_0 + a_1\frac{r}{s} + \cdots r_n\frac{a^n}{s^n} = 0.$$

Multiplicando ambos os termos da igualdade acima por s^n obtém-se:

$$f(\frac{r}{s}) = a_0s^n + a_1rs^{n-1} + \cdots a_{n-1}r^{n-1}s + a_nr^n = 0.$$

Assim,

$$\begin{aligned} -a_0s^n &= a_1rs^{n-1} + \cdots a_{n-1}r^{n-1}s + a_nr^n \\ &= r\left(a_1s^{n-1} + \cdots a_{n-1}r^{n-2}sa_nr^{n-1}\right) \end{aligned}$$

e

$$\begin{aligned} -a_n a^n &= a_0 s^n + a_1 r s^{n-1} + \cdots a_{n-1} r^{n-1} s \\ &= s\left(a_1 s^{n-2} + \cdots a_{n-1} r^{n-2}\right) \end{aligned}$$

As duas últimas equações acarretam $r|a_0 s^n$ e $s|a_n r^n$. Mas, MDC $(r, s) = 1$ implica MDC $(r^n, s) =$ MDC $(r, s^n) = 1$. Logo, $r|a_0$ e $s|a_n$. Podemos resumir este resultado na forma de um teorema.

Teorema 4.1. *(Teste da raiz racional) Seja* $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ *um polinômio com coeficientes inteiros. Se um número racional não nulo* $\frac{r}{s}$ *com MDC* $(r, s) = 1$ *é raiz de* $f(x)$*, então* $r|a_0$ *e* $s|a_n$*.*

Exemplo 4.1. As possíveis raízes em $\mathbb{Q}$ de $f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$ são da forma $\frac{r}{s}$ com $r \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ e $s \in \{\pm 1, \pm 2\}$. Assim,

$$\frac{r}{s} \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm\frac{1}{2}, \pm\frac{3}{2}\}$$

Pode-se verificar que -3 e $\frac{1}{2}$ são as únicas raízes racionais de $f(x)$. Usando o teorema do fator obtém-se:

$$f(x) = (x + 3)(x - \frac{1}{2})(2x^2 - 4x - 8).$$

Exemplo 4.2. As únicas raízes racionais possíveis do polinômio $f(x) = x^3 + 4x^2 + x - 1$ são ± 1. Mas, $f(1) = 5$ e $f(-1) = 1$. Logo, $f(x)$ não possui raízes em $\mathbb{Q}$. Como deg $f(x) = 3$ segue que $f(x)$ é irredutível sobre $\mathbb{Q}$.

4.3 O conteúdo de um polinômio

O contéudo de um polinômio não nulo $f(x) = a_0 + a_1 x + \cdots a_n x^n \in \mathbb{Z}[x]$ é o MDC de seus coeficientes. Um polinômio é dito primitivo

se possui conteúdo igual a 1.

Notação: $\text{cont}(f(x)) = \text{MDC } (a_0, a_1 \ldots, a_n)$.

O "set up" no estudo do conteúdo de polinômios reside no seguinte fato: se um primo $p \in \mathbb{Z}$ divide todos os coeficientes de um produto $f(x)g(x)$ de polinômios em $\mathbb{Z}[x]$ então p divide todos os coeficientes de $f(x)$ ou p divide todos os coeficientes de $g(x)$.

Teorema 4.2. *(Gauss) Seja $p \in \mathbb{Z}$ primo e $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots b_mx^m$ dois polinômios em $\mathbb{Z}[x]$ não nulos. Seja $h(x) = f(x)g(x) = c_0 + c_1x + \cdots c_{n+m}x^{n+m}$. Se $p|c_i$ $(0 \leq i \leq n+m)$ então $p|a_i$ $(0 \leq i \leq n)$ ou $p|b_i$ $(0 \leq i \leq m)$.*

Prova: (Redução ao absurdo) Suponha que existam i_0, j_0 tais que $p \not| a_{i_0}$ e $p \not| b_{j_0}$. Sejam a_r e b_s os primeiros coeficientes de $f(x)$ e $g(x)$ (a contar de c_0 e b_0), respectivamente, não divisíveis por p. Pela escolha de r e s, $p|a_i$ $0 \leq i < r$ e $p|b_j$ $0 \leq j < s$. Então,

$$c_{r+s} = a_0b_{r+s} + \cdots a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + \cdots a_{r+s}b_0$$

é tal que $p|c_{r+s}$ por hipótese e $p|a_0, \ldots, a_{r-1}, b_0, \ldots, b_{s-1}$ pela escolha de r e s. Logo, $p|a_rb_s$. Como p é primo (hipótese) devemos ter $p|a_r$ ou $p|b_s$, absurdo. $\square$

OBS 4.1. Se $cf(x) = g(x)h(x)$, $f(x), g(x), h(x) \in \mathbb{Z}[x]$, então $f(x) = \pm\tilde{g}(x)\tilde{h}(x)$ com $\tilde{g}(x), \tilde{h}(x) \in \mathbb{Z}[x]$, deg $\tilde{g}(x) =$ deg $g(x)$ e deg $\tilde{h}(x) =$ deg $h(x)$. Aplique a lei do cancelamento em domínios juntamente com o teorema anterior para todos os fatores primos de c.

4.4 Lema de Gauss

Dados $f(x) = x^4 - 4x^3 + 6x - 2$ e $g(x) = 5x^3 + 6x - 3$ temos $\text{cont}(f) = 1$ e $\text{cont}(g) = 1$. Assim, ambos f e g são primitivos. Por outro lado,

$$f(x).g(x) = 5x^7 - 20x^6 + 6x^5 + 3x^4 + 2x^3 + 36x^2 - 30x + 6$$

e $\text{cont}(fg) = 1$. Este resultado não é mera coincidência e sim uma regra. Se considerarmos dois polinômios primitivos, o produto será sempre primitivo. Em outras palavras, a noção de primitivo é preservada pelo produto. Este resultado é conhecido como lema de Gauss.

OBS 4.2. Se a é um inteiro positivo e $f(x) \in \mathbb{Z}[x]$ então $\text{cont}(af) = a.\text{cont}(f)$. Em particular, se $d = \text{cont}(f)$ então $\frac{1}{d}f$ é primitivo.

Teorema 4.3. *(Lema de Gauss) O produto de polinômios primitivos é um polinômio primitivo. Mais geralmente, o conteúdo do produto é o produto dos conteúdos.*

Prova: Sejam $f(x), g(x) \in \mathbb{Z}[x]$ primitivos e $d = \text{cont}(fg)$. Queremos provar que $d = 1$. Suponha $d \neq 1$. Existe ao menos um primo p tal que $p|d$. Por definição de MDC, p divide todos os coeficientes de fg. Pelo teorema 4.2, p divide todos os coeficientes de f ou p divide todos os coefientes de g. Logo, $p \mid \text{cont}(f)$ ou $p \mid \text{cont}(g)$, isto é, $p|1$, uma contradição. Assim, $d = 1$. Para finalizar, sejam $f(x), g(x) \in \mathbb{Z}$ polinômios quaisquer e d_1,d_2 seus respectivos conteúdos. Então, $\frac{1}{d_1}f$ e $\frac{1}{d_2}g$ são primitivos donde

$\left(\frac{1}{d_1}f\right)\left(\frac{1}{d_2}g\right) = \frac{1}{d_1 d_2}fg$ é também primitivo. Assim,

$$\begin{aligned}\text{cont}(fg) &= \text{cont}\left[d_1 d_2\left(\frac{1}{d_1 d_2}fg\right)\right] \\ &= d_1 d_2.\text{cont}\left(\frac{1}{d_1 d_2}fg\right) \\ &= d_1 d_2.1 = d_1 d_2 = \text{cont}(f)\text{cont}(g). \quad \square\end{aligned}$$

4.5 Irredutibilidade em $\mathbb{Q}[x] \Leftrightarrow$ irredutibilidade em $\mathbb{Z}[x]$

A equivalência acima precisa de algumas ressalvas. Primeiro, a noção de irredutibilidade é relativa e não absoluta. Por exemplo, 2 é um polinômio irredutível em $\mathbb{Z}[x]$, mas é unidade em $\mathbb{Q}[x]$ e $2x-4$ é redutível em $\mathbb{Z}[x]$, mas é irredutível em $\mathbb{Q}[x]$. Segundo, um polinômio com coeficientes em $\mathbb{Q}[x]$ não pode ser considerado um polinômio em $\mathbb{Z}[x]$. Deste modo, para a equivalência acima fazer sentido devemos considerar polinômios primitivos.

Seja $f(x) \in \mathbb{Z}[x]$ primitivo. Obviamente, irredutibilidade em $\mathbb{Q}[x]$ implica irredutibilidade em $\mathbb{Z}[x]$ (raciocine por contrapositiva!).

Suponha $f(x)$ redutível em $\mathbb{Q}[x]$, isto é, $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Q}[x]$ e $\deg g(x), \deg h(x) < \deg f(x)$. Existem inteiros a e b tais que $ag(x), bh(x) \in \mathbb{Z}[x]$. Então, $abf(x) = (ag(x))\,(bh(x))$ é uma fatoração de $abf(x)$ em $\mathbb{Z}[x]$. Denotando $c = ab$ e $\tilde{g}(x) = ag(x)$ e $\tilde{h}(x) = bh(x)$ temos $cf(x) = \tilde{g}(x)\tilde{h}(x)$. Segue da observação 4.1 que $f(x) = \pm\tilde{g}(x)\tilde{h}(x)$ com $\deg \tilde{g}(x) = \deg g(x) < \deg f(x)$ e $\deg \tilde{h}(x) = \deg h(x) < \deg f(x)$. Assim, $f(x)$ redutível em $\mathbb{Q}[x]$ implica $f(x)$ redutível em $\mathbb{Z}[x]$. Temos provado o seguinte:

Teorema 4.4. *Um polinômio primitivo em $\mathbb{Z}[x]$ é irredutível em $\mathbb{Z}[x]$ se e somente se é irredutível em $\mathbb{Q}[x]$.*

OBS 4.3. Dado $f(x) \in \mathbb{Q}[x]$, existe um inteiro c tal que $cf(x) \in \mathbb{Z}[x]$. Temos $f(x)$ redutível em $\mathbb{Q}[x]$ se e somente se $cf(x)$ irredutível em $\mathbb{Q}[x]$. Assim, com respeito à redutibilidade em $\mathbb{Q}[x]$ podemos sempre supor o polinômio em $\mathbb{Z}[x]$. Ademais, como redutibilidade é invariante pela noção de associados e sobre corpos sempre existe associado mônico (único) podemos também supor $f(x)$ primitivo. Pelo teorema anterior, $f(x)$ irredutível em $\mathbb{Z}[x]$ implica $f(x)$ irredutível em $\mathbb{Q}[x]$. Deste modo, se quisermos provar que um polinômio $f(x)$ em $\mathbb{Q}[x]$ é irredutível (em $\mathbb{Q}[x]$) é suficiente provar a irredutibilidade em $\mathbb{Z}[x]$ de um polinômio primitivo em $\mathbb{Z}[x]$ associado à $f(x)$ em $\mathbb{Q}[x]$. É neste fato que reside a importância de se elaborar critérios de irredutibilidade em $\mathbb{Z}[x]$.

4.6 Conclusão

Por meio do conceito de conteúdo de um polinômio com coeficientes inteiros, concluimos que o estudo dos irredutíveis em $\mathbb{Q}[x]$ está incluído no estudo dos irredutíveis em $\mathbb{Z}[x]$. Daí a necessidade de se obter critérios de irredutibilidade em $\mathbb{Z}[x]$.

RESUMO

Teste da raiz racional

> Se um número racional $\frac{a}{b}$, MDC$(a,b) = 1$, é raiz de $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ então $a|a_0$ e $b|a_n$.

O conteúdo de um polinômio

1. **Definição:** cont $(a_0+a_1x+\cdots+a_nx^n) =$ MDC $(a_0, \ldots, a_n)$.
2. **Polinômio primitivo:** polinômio de conteúdo 1.

3. **Teorema:** (Gauss) Se um primo p divide todos os coeficientes de um produto de polinômios então p divide todos os coeficientes de um dos fatores.

Lema de Gauss

$$\text{cont}(f(x)g(x)) = \text{cont}(f(x))\text{cont}(g(x)).$$

Irredutibilidade em $\mathbb{Q}[x]$ *versus* **Irredutibilidade em $\mathbb{Z}[x]$**

Para polinômios primitivos vale a equivalência

Irredutibilidade em $\mathbb{Z}[x] \Leftrightarrow$ Irredutibilidade em $\mathbb{Q}[x]$.

Consequência:

Seja $f(x) \in \mathbb{Q}[x]$ e $\tilde{f}(x)$ seu associado mônico em $\mathbb{Z}[x]$. Então, $\tilde{f}(x)$ irredutível em $\mathbb{Z}[x]$ implica $f(x)$ irredutível em $\mathbb{Q}[x]$.

PRÓXIMA AULA

Seguindo a motivação dos resultados obtidos nesta aula, buscaremos critérios de irredutibilidade em $\mathbb{Z}[x]$.

ATIVIDADES

ATIV. 4.1. Use o teste da raiz racional para escrever cada polinômio como um produto de polinômios irredutíveis em $\mathbb{Q}[x]$.

a) $3x^5 + 2x^4 - 7x^3 + 2x^2$.

b) $2x^4 - 5x^3 + 3x^2 + 4x - 6$.

ATIV. 4.2. Mostre que $\sqrt{p}$ é irracional para cada p primo.

ATIV. 4.3. Mostre que todo polinômio não nulo $f(x) \in \mathbb{Q}[x]$ pode ser escrito de maneira única na forma $f(x) = c\tilde{f}(x)$ com $c \in \mathbb{Q}$ e $\tilde{f}(x) \in \mathbb{Z}(x)$ primitivo. Conclua que todo polinômio em $\mathbb{Q}[x]$ possui um único associado mônico em $\mathbb{Z}[x]$.

ATIV. 4.4. Seja $f(x) \in \mathbb{Z}(x)$ primitivo. Mostre que se $f(x)$ é redutível em $\mathbb{Q}(x)$ então $f(x)$ é redutível em $\mathbb{Z}(x)$.

LEITURA COMPLEMENTAR

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.